How to Speed up Your Network

Troubleshooting a sluggish LAN can be a complex process, but there are a number of simple changes you can make to improve performance. We explain the main problem areas and their solutions.

By Simon Pride
System Administrator
Scient

This article is about getting the maximum performance from your LAN without changing your network hardware. The performance is achieved by optimising network traffic whilst still being able to support the business processes the computers in your enterprise are there to enable. It will consider systems with connections to two of the major LAN server systems in use today - Novell NetWare, and the various forms of Microsoft LAN networking.

Ethernet Configuration

One area where LAN performance can seem sluggish is where the rules of constructing Ethernet networks have been ignored or are not known. It is therefore useful to review these rules. Many enterprises that start with a handful of computers, and have the foresight to network them, will usually start with a single Ethernet hub (repeater) - possibly a cheap 8-port unit. Sooner or later the enterprise's growth will require more than eight hosts on the LAN, and that LAN will be extended. The easiest way to do this is by daisy-chaining hubs together, and for small networks this is indeed a valid strategy. However, there are some industry-determined rules about Ethernet networks, such as:

- The maximum length of a Thick Ethernet (10Base5) backbone is 500 metres.
- This backbone may be tapped to provide local network access at no more than 100 points.
- The maximum length of AUI cable from a tap point is 15 metres.
- The maximum length of a segment of Thin Ethernet (10Base2 or thinnet) is 185 metres.
- There can be no more than four repeaters (hubs) on a 10Base-T segment.
- The maximum length of cable from hub to network host is 100 metres.

You can break these rules, and your network will probably work, most of the time. However, if you carry on adding devices to a network over and above the official specs, you will find that performance degrades and strange errors occur at random times. These problems can often look very much like client configuration or hardware problems, and many hundreds of support hours have been wasted trying to troubleshoot problematic workstations when, in fact, the network infrastructure itself has been at fault.

Assuming your network infrastructure is within spec, we can move on to looking at the kinds of traffic on a network with a view to minimising inessential use.

Minimising Traffic

Traffic on LANs can be assigned to different categories which need different strategies to reduce their usage of available bandwidth. Some of the usage is barely optimisable - for example, the data sent when a workstation reads a file from a file server or sends a stream of data to a network print queue - but a good deal of LAN traffic is concerned with elements of housekeeping and can be reduced without affecting the business being done.

Far and away the most likely candidate for tuning on small to medium LANs is traffic caused by resource location. Windows networking, from the early days of LAN Manager to Windows NT, has always depended on the same resource location methods. In a Windows network, also known as an SMB network after

the upper-layer protocol Server Message Block underlying the system, resource location is dependent on computers known as “browsers”. The browsing mechanism is a significant consumer of LAN resources and any attempt to reduce browser traffic will deliver improved LAN performance. Note that, latterly, “browser” has two meanings, the more current and popular one being applied to World Wide Web clients. In this article, “browser” refers to the particular computer role as defined in Microsoft networking.

Browsers

A Windows network (typically a single subnet or segment) in a stable state has one computer called the Master Browser or Browse Master (Microsoft itself does not use one term consistently in its documentation), and one or more Backup Browsers. The role of the Master Browser is to collect the NetBIOS names of all computers on the subnet offering shared resources, and to forward a list of those names to the Backup Browsers. A Backup Browser’s role is to keep this list of names and to forward it to any workstation which is looking for networked resources (such as shares or shared printers).

When a workstation is switched on or rebooted, it sends a broadcast Server Announce datagram which is received by the Master Browser. The Master Browser registers the announcing workstation’s NetBIOS name and incorporates it into its browse list. By default, Backup Browsers interrogate the Master Browser every 12 minutes and retrieve the latest list of computers on the subnet, which they then store.

When a workstation needs to use a network resource, it first queries the Master Browser for a list of Backup Browsers; in response, the Master Browser returns the NetBIOS names of up to three Backup Browsers. The workstation then picks one of these three at random and asks it for a list of network shared resources. Only then does the list of networked machines appear in an Explorer window or an application’s file dialog box. Finally the workstation resolves the NetBIOS name of the host to a network address and contacts the host.

Figure 1 - Disabling MS client bindings to IPX on Windows NT.

Figure 2 - Disabling MS client bindings to IPX on Windows 95.

The description above is quite verbose, and the verbosity of the description parallels the verbosity of the network traffic needed to support this networking architecture. In a recent publication, Microsoft itself discloses that over 30% of its internal LAN traffic is made up of datagrams supporting browser conversations. Clearly, if browser traffic can be reduced, a significant amount of LAN bandwidth can be released for use.

Real-life Networks

So, can browser traffic be reduced without impairing network functionality? The answer will depend on the disposition of your network and, to a large extent, the culture of your organisation. The Microsoft networking world is designed to support a culture of autonomous, independent users and workgroups, sharing pieces of their work with each other and the enterprise at large, as and when the need arises. In this world, shared directories (shares) and even hosts come and go as the activities of the individuals and teams change. The onus is on the individual to browse the network resources and locate the shared resources that interest them, and the browse-oriented nature of Microsoft networking supports this.

Unfortunately for the IT professional, this is not how the vast majority of real-world networks are organised in enterprises. Instead, resources are centralised, typically with a small number of powerful and dedicated computers acting as servers, and a large number of client workstations using the shared resources on the server. Instead of individual users choosing whether or not to publish their work via individual shares from their workstation, functional groups have shared areas of file space on server volumes, with structured and managed access rights influencing how users may use other users’ information.

If your enterprise is full of bright, computer-literate, independent and mobile knowledge workers, perhaps the pure Microsoft model suits your users best. However, most of us inhabit the other world where resources are fixed for long periods of time, and the locations of those resources are well-known. In this world,

browsing is unnecessary and can be dispensed with. Login scripts can map drive letters to frequently used shares, and NT profiles can place network-appropriate printer objects in users' Printers folders. The typical user will still be able to access the resources needed to do their work, but the need to have browse lists of those resources available is eliminated.

TCP/IP Only

If your network is based around TCP/IP there is a further step you can take towards reducing traffic, one which is not available when using other protocols such as NetBEUI or IPX/SPX. Once a resource has been identified by its name, the workstation must still resolve that name to a network address. This is normally achieved by broadcasts, irrespective of the protocol in use; however, network clients from Windows for Workgroups 3.10 upwards can be set to use a NetBIOS name server, called a WINS server by Microsoft, to discover the TCP/IP address of any named server on the network.

WINS stands for Windows Internet Name Service, a service running on Windows NT Server which provides NetBIOS name-to-IP address resolution. WINS holds a database of names that have been registered with it by client workstations, together with their IP addresses. If a client workstation has been configured to use a WINS server, instead of sending a broadcast to all hosts on its subnet in order to resolve a name, it sends a few directed datagrams to the server and receives an individual response. This removes the need for all other hosts on the subnet to process broadcasts every time one of their number needs to resolve a name.

Removing Browser Traffic

Once the need for browsing is eliminated, you can progress to removing the capability of creating browser traffic from your users' computers. On Windows 95 and Windows 98 this is the File And Print Sharing option in Control Panel/Network/File And Print Sharing. Click the button File And Print Sharing, and uncheck the check boxes "I want to be able to give others access to my files" and "I want to be able to allow others to print to my printer(s)". Click OK and then OK again on the underlying Network dialog. You will have to reboot the computer before this takes effect.

In Windows NT the Server service is responsible for offering shared folders and printers to other users on the network, and is also responsible for announcing the presence of shared resources to browsers. In a managed network it is not needed on workstations or on application servers (such as database servers) which offer no shares or printers. To disable it, select Start/Settings/Control Panel/Network/Bindings. Highlight the Server service and click Disable. As ever, when making a change to the network configuration in Windows, you will need to reboot the workstation.

"There is a NetWare-specific UNC syntax which bypasses all other providers and goes directly to the NetWare provider, but works only with the NET USE command."

Browser Elections

If you must have a classical Microsoft browser-oriented network there are still steps you can take to reduce network traffic. The most significant of these is control of elections. Above, we referred to methods of NetBIOS resource location over an IP network using a NetBIOS name server - in that particular case a WINS server. In the absence of such a name service, Windows computers will use one of two other methods of name resolution: consulting a file local to each computer which maps IP addresses to NetBIOS names, or the use of broadcasts to identify computers with particular names.

Looking at the latter example first: as mentioned above, a Windows computer will contact its Browse Master to obtain a list of Backup Browsers, and then contact one particular Backup Browser to obtain a list of computers on its network. The process by which any individual computer becomes a Backup Browser is, however, one of the major causes of unnecessary network congestion.

Every time a computer running Windows networking boots up, it queries the network to find the address of the Master Browser. On a stable, mature network it will retrieve the Master Browser address and carry on with the networking

process as described above. However, under some circumstances the computer can fail to locate a computer it considers to be the Master Browser (this can be due to network errors or problems with NetBIOS name compatibility in mixed Windows for Workgroups 3.1x / Windows 9x / Windows NT networks).

In this situation it instigates a browser election to force the creation of a new Master Browser. It does this by issuing a broadcast datagram for each network to which it is connected, which includes the computer's criteria for becoming a Master Browser. Various aspects of the computer's status are included in this statement of criteria, from the operating system version down to the length of time the computer has been participating on the network.

In theory, what should happen next is for every computer on the segment to receive the election datagram and compare the criteria expressed in the datagram with its own. If its own criteria take priority over the ones in the election datagram it has received, it broadcasts its own election datagram with its superior criteria; if the datagram received has superior criteria to its own the computer falls silent and takes no further part in the browser election process. However, network delays and congestion can mean that a station which receives an inferior broadcast election datagram never "hears" a subsequent superior datagram, and instead replies to the previous inferior datagram with its own election datagram, triggering another torrent of datagrams from hosts with superior criteria to its own.

Election Storms

On large segments this can result in a "storm" of election broadcast datagrams raging across the network, and indeed this storm can become self-perpetuating - if enough traffic due to the election storm is present on the segment, that sheer amount of traffic itself will prevent the proper reception of downlevel browser candidates from receiving the superior datagrams that would cause them to fall silent. A browser election storm can therefore rage for an extended period on a segment until all stations have finally agreed on which station has the best criteria to be Master Browser.

Naturally, while these election storms are going on the ordinary business of the network is impaired. On a properly managed network the network administrator will take steps to minimise or eliminate browser elections. The baseline rule to be followed in these situations is to identify the computers that have the most static role in the network and to configure them to be the Browse Master and Backup Browsers, and to deny any other computer the ability to become any sort of browser.

For most networks the static computers will be the Windows NT servers, be they Primary or Backup Domain controllers or standalone servers (member servers in Microsoft networking jargon). These should be configured always to be the browsers, and any downlevel clients prevented. If your network does not have sufficient servers on each segment to fulfil Microsoft's recommended ratio of browsers to workstations (one browser per 12 computers), you should configure the most powerful workstations as Backup Browsers, and ensure they are always powered on and connected to the network.

Figure 3 - NT Network Services property sheet.

Forcing Browser Status

To force a Windows NT computer to be a browser, set the registry key HKLM / SYSTEM / CurrentControlSet / Services / Browser / Parameters / MaintainServerList to "Yes" (type REG_SZ).

To force a computer always to be the domain Master Browser, set HKLM / SYSTEM / CurrentControlSet / Services / Browser / Parameters / IsDomainMaster to a REG_SZ value of TRUE.

To prevent a Windows computer from becoming a browser, set the same key on Windows NT to "No". For Windows 9x, set HKLM / SYSTEM / CurrentControlSet / Services / VxD / VNETSUP / MaintainServerList to "No", or alternatively go to Control Panel / Network / File And Print Sharing... / Advanced. Select "Browse Master" from the "Property" list box and, while it is selected, set "Value" from the combo box on its right to "Disabled".

To prevent a Windows for Workgroups computer from participating in browser elections, locate the [Network] section in SYSTEM.INI, add a key called "MaintainServerList" and assign it a value of "No".

Browse Lists

Once you have stabilised the browser election issue, you can think about reducing another component of browsing, which is the distribution of browse lists to Master Browsers. In an NT-based network, a Primary Domain Controller will assume the role of Domain Master Browser. Master Browsers attempt to contact the Domain Master Browser every 12 minutes to update their browse lists. However, if the Domain Master Browser sees that the Master Browser is connecting from a different subnet, it will establish another connection back to the browser in order to update its own browse list with the server data that browser has collected.

Stable, managed networks do not need to update their list of networked resources as frequently as every 12 minutes. Values of one or two hours are much more appropriate and will cut browser traffic drastically without impairing functionality. To change the browser update interval on Domain Master Browsers, set the registry key HKLM/System/CurrentControlSet/Services/Browser/Parameters/MasterPeriodicity to a REG_DWORD value of N seconds. The default is 720 seconds (12 minutes), but values of up to 86400 seconds (24 hours) are not inappropriate for a stable network.

Reduce Protocols

You may have transport protocols on your network which are not required for your business. This is often encountered when an enterprise has Windows 9x workstations on its network since, by default, Windows 95 and 98 will install the NetBEUI and IPX/SPX Compatible Protocol when networking is configured. Many enterprises are concentrating on TCP/IP as their sole transport protocol, and IT staff will usually add and configure TCP/IP later.

"The Microsoft networking world is designed to support a culture of autonomous, independent users and workgroups, sharing pieces of their work with each other and the enterprise at large."

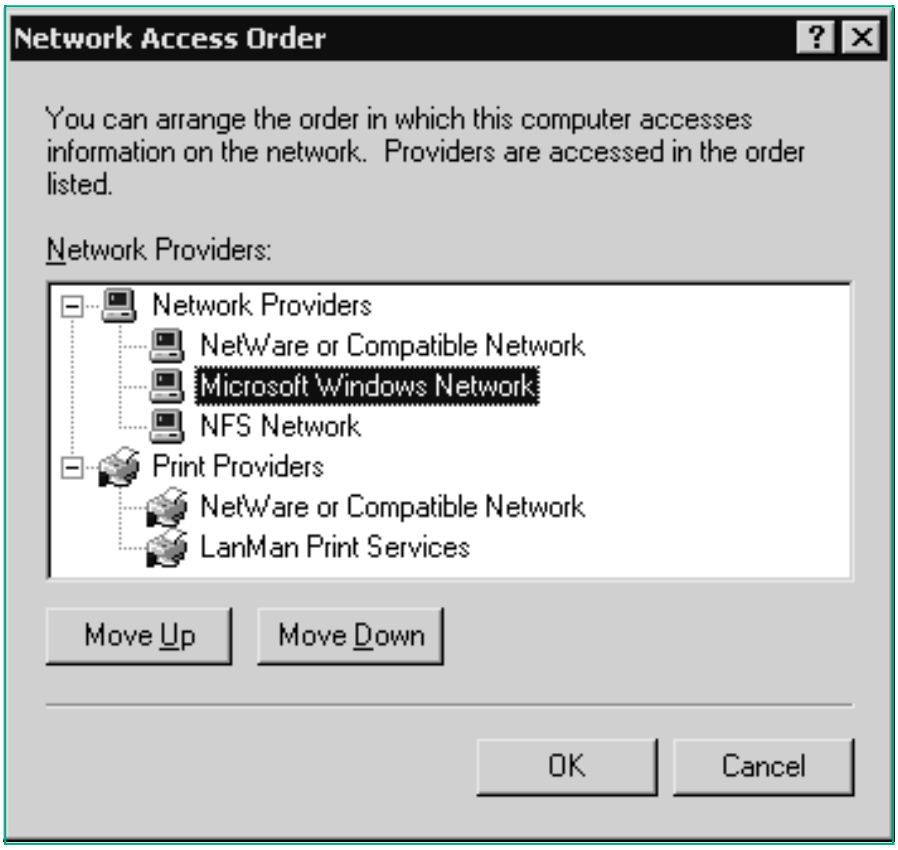

Figure 4 - Setting network access order on Windows NT.

In many cases, the two legacy protocols are left installed even when they are not needed. This ought not to be a problem; after all, if a protocol is not used in the enterprise it cannot usually do any harm. However, once again we come up against the verbose and chatty nature of Microsoft networking and its effect on network traffic.

A computer which has Microsoft networking installed but has been subject to no further configuration, and which has all three of the usual protocols installed (NetBEUI, IPX/SPX and TCP/IP), will use NetBIOS networking on each installed protocol. That is, it will announce itself to browse masters, take part in browser elections and exchange browse lists over each of the three installed protocols. A browser election storm over IP is bad enough without the addition of two further election disputes happening over IPX and NetBEUI. All of these datagrams must be transported over Ethernet, where, irrespective of transport protocol, a datagram is a datagram. The more datagrams stations put onto the network, the greater is the likelihood of collisions, and greater the level of congestion on the network.

There are two approaches to this problem, depending on whether you need to use the legacy protocols or not. Actually, in practice the choice is whether to run IPX/SPX or not - if your enterprise is using any other transport protocol, you don't need NetBEUI. NetBEUI is a simple and fast protocol but has none of the facilities which are required in a modern internetworking transport, and should only be used on small LANs (of fewer than 150-200 hosts) where neither connectivity across different LAN segments nor Internet access are needed.

IPX/SPX is needed if your users' Windows workstations need to connect to NetWare 3.x or 4.x servers, 5.x servers that are not fully IP-based, or if you have NT servers which for some reason are providing services over IPX/SPX. If you need to retain IPX/SPX connectivity but want to cut down the network traffic incurred by Microsoft networking broadcasts over IPX, you need to unbind NetBIOS networking from the IPX/SPX protocol. Note that this will not affect NetWare client functionality, as traffic between workstation and Novell server does not use NetBIOS.

Unbinding NetBIOS

To unbind NetBIOS from IPX/SPX: On Windows 9x, select Control Panel/Network/Configuration and highlight IPX/SPX-compatible Protocol. Click Properties, choose the Bindings tab and uncheck (unselect) Client For Microsoft Networks and File And Printer Sharing For Microsoft Networks. When you have completed these steps the Bindings property sheet should look like Figure 1. Click OK and then click OK on the Network dialog. You will be prompted to reboot the computer.

On Windows NT go to Control Panel/Network/Bindings/NetBIOS Interface. Click the plus icon next to NetBIOS Interface to display the services bound to that protocol. Locate NWLink NetBIOS and select it, then click the Disable button. Repeat these steps for the binding of both NWLink NetBIOS and NWLink IPX/SPX Compatible Transport to the Server and Workstation services. When you have made the changes the Bindings property sheet should look like Figure 2. When complete, click OK, and reboot the computer as prompted.

"By far and away the most likely candidate for tuning on small to medium LANs is traffic caused by resource location."

If you don't need IPX/SPX at all, you can simply remove it. On Windows 9.x go to Control Panel/Network/Configuration and highlight IPX/SPX-compatible Protocol. Click Remove (dependent clients and services will be removed automatically) and then reboot the computer when prompted. On Windows NT go to Start/Settings/Control Panel/Network/Services/Client Service For NetWare and click Remove. Then go to the Protocols tab, highlight NWLink and click Remove there too. Click OK and reboot the computer when prompted.

Network Access Order

Windows 9x and NT are not particularly intelligent when it comes to locating on which type of network server a resource is located. When Windows receives a request to access a resource on a named server, it tries each network that is installed in order, using whatever name resolution methods are appropriate to

that network, until the server is found. This can impact performance, since the next network is not tried until Windows has established that the resource is not present on the current network. Nor does this information appear to be cached between requests, so every time a network operation is required Windows looks for the server again.

You can influence the order in which your users' workstations look for servers, so that if your environment is predominantly one using NetWare servers IPX/SPX is tried first, and TCP/IP first if you are using predominantly Windows NT.

On Windows 9x this procedure is relatively difficult compared with NT's GUI-based approach (see below), involving registry editing. It is perhaps prudent to repeat here Microsoft's warning that mistakes made while editing the registry can render Windows unusable, and that the cautious system administrator will always have taken a backup of the registry before beginning. As Microsoft says: *"Note that you should make a backup copy of the registry files (SYSTEM.DAT and USER.DAT) before you edit the registry. WARNING: Using Registry Editor incorrectly can cause serious problems that may require you to reinstall Windows 95. Microsoft cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk."*

That said, in order to alter the network access order start REGEDIT.EXE and locate the keys HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/-MSNP32/NetworkProvider (for Microsoft Networking) and HKEY_LOCAL_-MACHINE/System/CurrentControlSet/Services/NWNP32/NetworkProvider (for NetWare networks). Within each key there is a value called CallOrder. The default CallOrder value for Novell NetWare is 00 00 00 20, and the default value for Microsoft networking is 00 00 00 40. A network provider with a lower call order value will be tried before one with a higher value. This means that Windows will look for a resource on the Novell NetWare network first, which is a sensible default given that, where NetWare is used, it does tend to be the predominant network.

However, if your enterprise is migrating to NT or has a few NetWare servers for specialist duties (for instance, several financial systems are implemented as NLMs), you can reverse the two call order values so that Microsoft networking is consulted first.

On Windows NT go to Control Panel/Network/Services/ and Click the Network Access Order button (see Figure 3). Note that this button is only displayed when Client Services for NetWare (CSNW) for NT or Gateway Services for NetWare (GSNW) are installed. NT 4 has separate access orders for file and print services, whereas earlier versions treated all services on the network alike. This is useful if, for instance, your applications are largely based on NT but you use legacy NetWare printing. To set the order for each class of network usage, click on either Network Providers or Print Providers, then highlight the network provider you wish to promote to be the first to service file or print requests, and use the Move Up and Move Down buttons to set the desired order (see Figure 4). Click OK to finish. You will need to reboot the computer to effect the changes.

"WINS stands for Windows Internet Name Service, a service running on Windows NT Server which provides NetBIOS name-to-IP address resolution."

NET USE

There is a way of quickly connecting to NetWare resources which is documented in Microsoft Knowledgebase article Q177602 (on the Web at **support.microsoft.com/support/kb/articles/q177/6/02.asp**). The standard way of specifying any network resource on Windows is to use its Universal Naming Convention (UNC) path, of the form: \\SERVER\SHARE\SUBDIRECTORY\FILE. On Windows 9x and NT this works both for Windows and NetWare resources; in NetWare's case the traditional specification of SERVER/VOLUME:DIRECTORY/SUBDIRECTORY/FILE maps to \\SERVER\VOLUME\DIRECTORY\-SUBDIRECTORY\FILE.

These UNC paths can be used either in Explorer's Map Network Drive dialog, in a NET USE command in the console window, or in the Run command from the Start menu (running a UNC path opens a My Computer window on the specified resource). However, unless you have optimised your network provider order for

NetWare networks as described above, you will still have the annoying wait while Windows consults the Microsoft networking provider to locate the desired server. There is a NetWare-specific UNC syntax which bypasses all other providers and goes directly to the NetWare provider, but works only with the NET USE command. The standard syntax is:

```
NET USE <drive letter>: \\SERVER\VOLUME
```

The NetWare-specific syntax is:

```
NET USE <drive letter>: SERVER\VOLUME:
```

Note that there is no preceding UNC double slash and a colon after the volume name. On my office network, which has mixed Microsoft, NetWare and NFS networking, the standard syntax of the command took seven seconds to complete, whereas the NetWare-specific form completed immediately.

Other Trafficky Services

If optimising the housekeeping elements of essential services does not produce the benefit you are looking for, check to see if computers on the network are offering unnecessary services which are claiming bandwidth. If users have been allowed to install their own copy of Windows NT Workstation, or if it has been installed by inexperienced IT staff, it is possible that a Windows NT Workstation is running the personal version of Microsoft's Internet Information Server Web Server (IIS), called Microsoft Peer Web Services. Although this generates no network traffic by itself, if users have been tempted to put up their local Web pages then bandwidth will be consumed by workers browsing the local server.

In several organisations where Web access is limited to approved sites I have seen Web servers on personal workstations which provide "mirrors" of commercial sites not normally available to other workers in the organisation; one example was a fairly complete copy of the UK Manchester United football team's home site. Such sites are graphic-rich and attractive to many workers, consuming both network bandwidth and workers' time in office hours.

Detecting unauthorised Web servers is relatively easy, given that few amateur users ever move the server from its default TCP port of 80. A script which iterates through a list of the organisation's IP addresses and telnets to port 80 on each address is sufficient. If no server is running, the response "connection refused" should be received; if a server is running it will announce itself on connection. These responses can be recorded to a log file and analysed later by hand or program.

Conclusion

Carrying out some or all of the optimisations in this article can lead to significant improvements in performance. Where they do not improve performance there are likely to be other factors creating bottlenecks, such as a saturated LAN segment (too much traffic for the hardware to cope with), a faulty Ethernet card emitting spurious packets, or an overworked bridge or router. Diagnosis of these normally requires specialist expertise or equipment.

"Mistakes made while editing the registry can render Windows unusable; the cautious system administrator will always have taken a backup of the registry before beginning."

PCNA

New Reviews from Tech Support Alert

Anti-Trojan Software Reviews

A detailed review of six of the best anti trojan software programs. Two products were impressive with a clear gap between these and other contenders in their ability to detect and remove dangerous modern trojans.

Inkjet Printer Cartridge Suppliers

Everyone gets inundated by hundreds of ads for inkjet printer cartridges, all claiming to be the cheapest or best. But which vendor do you believe? Our editors decided to put them to the test by anonymously buying printer cartridges and testing them in our office inkjet printers. Many suppliers disappointed but we came up with several web sites that offer good quality cheap inkjet cartridges with impressive customer service.

Windows Backup Software

In this review we looked at 18 different backup software products for home or SOHO use. In the end we could only recommend six though only two were good enough to get our “Editor’s Choice” award

The 46 Best Freeware Programs

There are many free utilities that perform as well or better than expensive commercial products. Our Editor Ian Richards picks out his selection of the very best freeware programs and he comes up with some real gems.